SENSITIVE IMACS DATA ELEMENTS

Portal Considerations

SENSITIVE DATA ELEMENTS

IMACS Access Control

User access to IMACS data is controlled by the IMACS application

Access from application to database is controlled by Oracle Role-based security scheme which is controlled by IMACS DB tables

IMACS application determines the DMISAs a user can see and work on.

IMACS should be accessed through the IMACS application or a tool that can implement the same

SENSITIVE DATA ELEMENTS

IMACS database is a relational database

DMISA data is stored in a set of 78 tables.

Tables are related to each other through a system IMACS application generated common reference numbers as well as organizations, DODAACs, User-Ids, etc.

A table set is used to connect the user account and the reference number.

This mechanism determines who can see what DMISAs.

Implication

If a user has the ability to access IMACS through a method other than the IMACS application they will have the ability to view all the DMISAs by ignoring the security tables

SENSITIVE DATA ELEMENTS

- **PRICING DATA**
- **FUNDING DATA**
- **SELECT MISMATCH RECORDS**
- **REQUIREMENTS**

SENSITIVE DATA ELEMENTS

- **Conclusion**
  - If a user has the ability to access IMACS through a method other than the IMACS application they will have the ability to view all the DMISAs and associated data by ignoring the security tables and security built into the IMACS application.
  - IMACS should be accessed through the IMACS application or a software application that can implement the same security mechanisms as IMACS.

SENSITIVE IMACS DATA ELEMENTS

Portal Considerations